IN THE U.S. PATENT AND TRADEMARK OFFICE

Appellant:	Abbas BAGASRAWALA
Application No.:	09/771,406
Art Unit:	2145
Filed:	January 26, 2001
Examiner:	Jeffrey R. Swearingen
For:	INTERNET PROTOCOL SECURITY FRAMEWORK UTILIZING PREDICTIVE SECURITY ASSOCIATION RE-NEGOTIATION
Attorney Docket No.:	29250-002065/US

APPELLANT'S BRIEF ON APPEAL UNDER 37 C.F.R. §41.37

MAIL STOP APPEAL BRIEF - PATENTS
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

August 31, 2005

TABLE OF CONTENTS

APPELLANT'S BRIEF ON APPEAL UNDER 37 C.F.R. §41.37

I. REAL PARTY IN INTEREST:

The real party in interest in this appeal is Lucent Technologies Inc. Assignment of the application was submitted to the U.S. Patent and Trademark Office on January 26, 2001, and recorded on the same date at Reel 011498, Frame 0473.

II. RELATED APPEALS AND INTERFERENCES:

There are no known appeals or interferences that will affect, be directly affected by, or have a bearing on the Board's decision in this Appeal.

III. STATUS OF CLAIMS:

Claims 1-20 are pending in the application, with claims 1, 9 and 18 being written in independent form.

Claims 1-20 remain finally rejected under 35 U.S.C. §103(a) and are being appealed.

IV. STATUS OF AMENDMENTS:

A Request for Reconsideration ("Request") was filed on July 20, 2005. In an Advisory Action dated August 5, 2005, the Examiner stated that the Request was considered but did not place the application in condition for allowance.

V. SUMMARY OF CLAIMED SUBJECT MATTER:

The present invention relates generally to the field of securing data using the Internet Protocol Security (IPSEC) framework as proposed by the Internet Engineering Task Force (IETF).

(i.) Overview of the Subject Matter of the Independent Claims

The present application contains independent claims 1, 9 and 18. Claims 1 and 9 relate to the prediction of "a specific quantity of communication traffic between network elements" while claim 18 is related to predicting the "expiration" of "quantity based security associations" between network elements.

To carry out the prediction features of the invention, claims 1 and 9 of the present invention require the prediction of exchanges of a "specific quantity of communication traffic between network elements" by, among other things, "calculating a weighted traffic flow per usage for a given network element and a comparison of "the value of said weighted traffic flow usage with a remainder value of said specific quantity of communication traffic yet to be processed." Claim 18 adds the feature that the traffic may be a so-called "security association" (SA).

Support for the features in these independent claims can be found at least on pages 2-4 of the specification.

In addition, specific embodiments of the independent claims are also discussed on pages 5-9 of the specification.

(ii.) Additional Text from the Specification in Support of the Claims

To secure data over the Internet, the Internet Engineering Task Force (IETF) has recommended a set of protocols for the Internet Protocol (IP). These suites of secure protocols are referred to as Internet Protocol Security (IPSEC) protocols. IPSEC is a developing standard for security at the network or packet processing layer of network communication. Earlier security approaches had inserted security at the application layer of the communications model. IPSEC is especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A significant

advantage of IPSEC is that security arrangements can be handled without requiring changes to individual user computers.

The IPSEC protocols rely on keys to encrypt and decrypt the data. Two parties wishing to exchange data securely using IPSEC exchange IPSEC keys between them. The secure exchange of IPSEC keys is a major factor in determining the security and the integrity of a whole system. Other factors include the strength of crypto-algorithm (DES, 3DES), procedures, etc. (specification, page 1).

For large scale deployment of IPSEC and automatic exchange of keys between parties the IETF has defined a key exchange protocol known as the IKE (Internet Key Exchange). The IKE allows two parties to exchange IPSEC keys securely and automatically over the Internet. The IPSEC keys are exchanged by IKE by negotiating Security Associations (SA's) between the two parties. Security Associations (SA's) are simplex connections that afford security services to the traffic being carried. In other words, two sides wishing to communicate using IPSecurity (as defined by the IETF) negotiate and have Security Associations among them. The SA's specify the security parameters that should be used to communicate with the other parry. For bi-directional communication, each party typically has two SA's - incoming and outgoing. For added security (to avoid key compromise) and to prevent crypto analysis of the data transferred, RFC 2401 (the IPSEC RFC), recommends that an SA be valid for only a short period of time (e.g. 20 minutes) and that new keys should be exchanged at regular intervals. Accordingly, two parties need to renegotiate another set of security associations (SA's) if they wish to continue the exchange of data after the previous SA expires. The IPSEC RFC recommends two types of units to specify the life of the SA, i.e., time and/or bytes of data transferred. Thus, if the SA life is specified as 10 Mbytes then the two parties can exchange up to 10 Mbytes of data using the current SA. To send more data, the two parties should negotiate another set of SA's for every 10 Mbytes of data.

RFC 2401 specifies the SA life in time and bytes. When a SA life is specified in time units, in order to continue to send data, an initiator system has to renegotiate another set of SA's after the SA lifetime expires. While a new SA is being renegotiated, no data can flow. To prevent data flow interruption, often a system designer anticipates the expiration of a current SA. Before the current SA expires, the initiator system starts renegotiation of new SA's such that new SA's are available as soon as the current SA's expire. This prevents data flow interruptions.

The lifespans of SA's based on time units are relatively easy to renegotiate in advance. This is because the system designer can safely assume the time it might take to negotiate a set of SA's. Based on the time to renegotiate a new SA and the time left before the old SA expires, the system designer can compute the time the system can start new SA negotiations and thus prevent data interruptions. For example, if a current SA expires at T seconds and if it takes 15 seconds to negotiate a set of SA (worst case), then the system can start renegotiation T-15 seconds before the current SA expires and thus preventing data loss/interruptions (specification, pages 1-2).

When SA's are specified with life units based on bytes, it is not easy for a system to predict when the SA is going to expire. This is because the data flow is not always uniform. The Internet data flow is bursty in nature. That is, there could be a burst of data flow between the two systems followed by a lull and another burst. Predictability is extremely important in high-speed data communication systems where any interruption in the flow of data occurring due to SA re-negotiation can cause loss of lot of data. A need therefore exists to accurately predicting the expiry of SA's based in bytes.

The present invention is a methodology for predicting when current sets of encryption keys used in a high speed data network are about to expire. The invention allows network elements of a communication system to re-negotiate

new sets of keys well in advance so as to prevent interruptions in communications traffic flow.

In accordance with one exemplary embodiment of the invention, a weighted traffic flow per usage for a given network element is calculated on a periodic basis. The value of the weighted traffic flow per usage is compared with a remainder value of a specific quantity of communications traffic yet to be processed by the network element. If the remainder value is less than the weighted traffic flow value, an indication is given to the appropriate network element to renegotiate a new set of keys (specification, pages 2-3).

Fig. 1 (Appendix B) shows two computer systems which couple to one another for communications purposes over the public Internet. Although the present invention is illustrated in the context of a connection over the public Internet, it would be understood that the present invention could be utilized to enhance secure communications connections over substantially any type of communications network. In the exemplary embodiment of Fig. 1, a first endpoint computer system (system A) 10 and a second endpoint computer system (system B) 20 are configured to send data securely using IPSEC over the Internet communications network 30. As discussed in the background, to IPSEC is a developing standard for security at the network or packet processing layer of network communication. IPSEC is especially useful in the implementation of virtual private networks and for remote user access through dial-up connection to private networks. A significant advantage of IPSEC is that security arrangements can be handled without requiring changes to individual user computers.

In the embodiment of Fig. 1, system A 10 wishes to send communications traffic to system B 20. Accordingly, system A 10 is considered to be the initiator and system B 20 is considered to be the responder. In accordance with the subject matter of the present invention, the responder (system B) 20 has been configured to negotiate IPSEC keys with a limit, for

example, of 100 Mbytes. As the communication progresses, the initiator and the responder negotiate and exchange a set of keys with a limit of 100 Mbytes of data. The keys are discarded once the limit is reached. Thus, if system A 10 wants to continue sending more data to system B 20 beyond the 100 Mbyte limit, then system A 10 has to renegotiate another set of keys with system B 20. This allows system A to send the next 100 Mbytes. It is assumed for the purposes of this discussion that both systems A and B are systems that can renegotiate new keys without causing any interruptions in the traffic flow. Although highly desirable, such capability is not necessary for implementation of the present invention (specification, page 4).

For security associations (SA's) limited by an amount of traffic, e.g. bytes, a predictive algorithm in accordance with the present invention is used to evaluate when a new SA should be negotiated in order to avoid an interruption in data flow. A significant advantage of the present invention is that it is accurate and simple to implement without affecting performance of the system. As had been discussed in the background, due to the bursty nature of Internet traffic, it is not enough to compute the average flow of bytes for a given time period. The average method calculates the average number of bytes that were processed by a SA per period. For example, if for the SA during period TI 10 Mbytes of data was processed and during period T2 40 Mbytes of data was processed, then the average data processed per period is (10 + 40)Mbytes/2 periods = 25 Mbytes. This is different than an improved measurement technique which is presented in accordance with the present invention.

The improved measurement technique according to the present invention is to compute the average traffic processed per SA usage for a given time period. This is also called weighted traffic flow per usage. This is done by keeping track of how often the SA was used for a given time period and how many bytes were processed in the same period. By taking an average of the

number of times the SA was accessed and the average number of bytes per usage a computer system can accurately predict when the SA will expire. This is called the weighted average of SA usage per access. Thus, with respect to . the exemplary network of Fig. 1, the initiator system (e.g., system A 10), can renegotiate another set of SA's such that there are no traffic flow interruptions.

Referring to Fig. 2 (Appendix C), an exemplary flow diagram 200 of the present invention for the calculation of the weighted average of SA usage per access is shown. As would be understood by a person skilled in the art, in an exemplary form of the invention, the negotiations would be performed by the endpoint systems, each of which includes a digital processor. As would be understood, the steps of the present invention will be embodied in software stored in memory of the endpoint systems, which is accessible by the digital processor. The invention could also be implemented in hardware, as would be understood (specification, pages 4-5).

In accordance with the flow diagram of Fig. 2, certain calculations are performed in accordance with the present invention methodology during every period. The calculation period is selectable according to parameters that would be known by a system's manager of a user system, for example, 15 seconds. A main criterion for selection of the time period is that the time period be smaller than the smallest known time block for transmitting the specified amount of data. This point is illustrated latter in the application by the exemplary calculation. In general, the time period will be chosen so that at least multiple re-negotiation calculations would be accomplished during the span of the smallest known time block. An exemplary time period for a system having a 100 Mbyte SA usage limit for the exemplary system of Fig. 1 may be 15 seconds.

With respect to Fig. 2, after a suitable period has been determined, the calculation begins at the Start box 210. As a first calculation during each time period, at box 220, an average use of a given Security Association is

determined. The calculation for average use of SA per period is equal to the total number of times the SA was used divided by the number of periods. The number of periods is counted from the time the SA was first negotiated. This number is updated at least at every increment in period. For example when utilizing 15 second periods, at time T0, the number of periods equals 0. After 15 seconds, the number of periods is 1 and at the end of 30 seconds is 2 and so on.

A decision box 230 is next entered to determine whether the SA has been used during the current period. If the SA was used during the period, the "Yes" path is followed to the next processing box 240. If the SA was not utilized during the current period, the "No" path is followed and the average bytes per use equal zero (box 280). The output of box 280 then loops to the input of box 250. In an alternative embodiment, the program could also loop back toward box 220 to begin another calculation of average use per period (specification, pages 5-6).

If the "Yes" path is followed from the decision box, the processing box 240 is entered. A calculation to determine the average number of bytes per use is performed. This value equals the number of bytes processed by SA divided by the number of times the SA was used.

Following the "Yes" path, a computation at processing box 250 is next completed to determine how much "time" remains before another SA must be negotiated. This value, referred to as "Remain" is equal to the SA life in bytes minus the number of bytes processed by the SA. The final calculation of the methodology of Fig. 2 is to determine whether the value of "Remain" is less than the average use of SA per period multiplied by the average bytes per use (value "X"). This comparison takes place at decision box 260. If the value of "Remain" is less than the average use of SA per period multiplied by the average bytes per use (value "X"), then a new SA is to be negotiated with the responder system (box 270). On the other hand, if the value of X is greater

than the value of "Remain", the SA predictor feature remains idle or sleeps until the beginning of another calculation in the same period. The calculation will also renew at the beginning of each new period (specification, pages 6-7).

The pseudo-code for the SA predictive renegotiation scheme is as follows:

In each period, compute:

avg_use_of_SA_per_period = number of times SA was used/number of periods.

IF SA was used then

avg_bytes_per_use = # of bytes processed by SA/# of times SA was used.

else

avg_bytes_per_use = 0;

Now compute how much time before we negotiate another SA.

remain = SA life in bytes - # of bytes processed by the SA

IF remain < (avg_use_of_SA_per_period*avg-bytes_per_use)

then negotiate another SA

ELSE

Sleep till next time period.

In order to further illustrate the present invention, a sample calculation utilizing the methodology of the present invention will be explained in connection with a sample communications flow. Referring to Fig. 3, a graphic illustrating an exemplary burst traffic flow is shown for communications traffic occurring between two endpoints over three different time periods. Within the first period (end of Tl), 10 Mbytes are processed. The first period (TI) is followed by a burst of 50 Mbytes during T2. T2 is followed by a lull of 10 Mbytes during T3.

Fig. 3 (Appendix D) also illustrates the number of times that the SA is used. Note that the number of times the SA is used is the same as the number of packets processed (encrypted or decrypted) by the SA. Dividing the number

of bytes processed by the SA by the packet size derives this number. In practice, the number is updated for each packet that is processed. With regard to the instant calculation, assumptions are made for a packet size of 1000 bytes, and a SA limit of 100 Mbytes (10^6 bytes) (specification, pages 7-8).

Taking the above information into account, it can be seen that for the sample communications flow of Fig. 3, the sample calculations utilizing the methodology of the present invention are as follows:

End of Tl Calculation:

Total Period Tp = 1, Total Bytes Tb = $10 * 10^6$, Total SA Usage Tu = $10 * 10^3$

1. Avg_use_of_SA_per_period Ab = Tu/Tp = $10 * 10^3$
2. Avg_Bytes_per_use Ab = Tb/Tp = 10^3
3. Remainder, R = 100 - 10 = $90 * 10^6$
4. Since R > (1) * (2) → No SA is negotiated

End of T2 Calculations:

Total Period Tp = 2, Total Bytes Tb = $50 * 10^6$, Total SA Usage Tu = $50 * 10^3$

1. Avg_use_of_SA_per_period Au = Tu/Tp = $25 * 10^3$
2. Avg_Bytes_per_use Ab = Tb/Tu = 10^3
3. Remainder, R = 100 - 50 = $50 * 10^6$
4. Since R> (1) * (2) → No SA is negotiated

End of T3 Calculations:

Total Period Tp = 3, Total Bytes Tb = $60 * 10^6$, Total SA Usage Tu = $60 * 10^3$

1. Avg_use_of_SA_per_period Au = Tu/Tp = $20 * 10^3$
2. Avg_Bytes_per_use Ab = Tb/Tu = $3 * 10^3$
3. Remainder, R = 100 - 60 = $40 * 10^6$
4. Since R < (1) * (2) → A new SA is negotiated

Based on the above, it can be seen that a new SA is negotiated at the end of period T3. It should be noted that for the same traffic pattern, but instead

using the "average bytes" method, no SA would have been negotiated at the end of T3. If in T4 period a burst of traffic of 50 Mbytes was received then the SA would expire (limit of 100 Mb) and thus a new SA would have to be negotiated which would result in loss of data while a new SA is negotiated. Accordingly, a significant advantage of the present invention of prior art methodologies is illustrated (specification, pages 8-9).

The present invention predictive SA renegotiation algorithm is accurate in predicting the SA expire time on different types of traffic, e.g., continuous steady stream of data (constant bandwidth) and/or bursty data patterns. A unique feature of the SA predictive algorithm is its accuracy and simplicity without affecting the performance of the system. The present invention predictive algorithm is also independent of the crypto-algorithm used for encrypting the traffic.

The SA predictive algorithm can be used in all systems supporting secure traffic using IPSEC standards. The algorithm is independent of the crypto-algorithm used in encrypting the traffic itself. The algorithm is also generic such that it can be used in traffic prediction especially in burst traffic common to the Internet.

The present invention methodology has other applications of use, besides IPSEC applications over the public Internet. Examples of other possible applications include Traffic Monitoring and Network Management Applications. Traffic management applications can use the predictive algorithm to predict and identify randomly occurring patterns. For example, the number of telephone calls or highway traffic pattern. Network Management Applications can use the predictive algorithm to monitor data and predict usage of network components. For example, if a modem banks are deployed to accept calls which are arriving randomly, then using the present invention, the application can predict when the modem banks will be saturated and can automatically add additional capacity (specification, page 9).

The foregoing description merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements, which, although not explicitly described or shown herein, embody the principles of the invention, and are included within its spirit and scope. Furthermore, all examples and conditional language recited are principally intended expressly to be only for instructive purposes to aid the reader in understanding the principles of the invention and the concepts contributed by the inventor to furthering the art, and are to be construed as being without limitation to such specifically recited examples and conditions. Moreover, all statements herein reciting principles, aspects, and embodiments of the invention, as well as specific examples thereof, are intended to encompass both structural and functional equivalents thereof. Additionally, it is intended that such equivalents include both currently known equivalents as well as equivalents developed in the future, i.e., any elements developed that perform the same function, regardless of structure.

In the claims hereof any element expressed as a means for performing a specified function is intended to encompass any way of performing that function including, for example, a) a combination of circuit elements which performs that function or b) software in any form, including, therefore, firmware, microcode or the like, combined with appropriate circuitry for executing that software to perform the function. The invention as defined by such claims resides in the fact that the functionalities provided by the various recited means are combined and brought together in the manner which the claims call for. Appellant thus regards any means which can provide those functionalities as equivalent as those shown herein. Many other modifications and applications of the principles of the invention will be apparent to those skilled in the art and are contemplated by the teachings herein. Accordingly, the scope of the invention is limited only by the claims.

Appellant respectfully notes that the above summary of the invention, including any indication of reference numerals, drawings, figures, paragraphs, page numbers, etc. (collectively referred to as "descriptions" of the application) have been provided solely to comply with the U.S. Patent and Trademark Office's rules concerning the appeal of the claims of the present application. As such, the descriptions above are merely exemplary and should not be construed to limit the claims of the present application in any way whatsoever.

VI. <u>GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL:</u>

Appellant seeks the Board's review of the rejection of claims 1-20 under 35 U.S.C. §103(a).

VII. <u>ARGUMENTS:</u>

Claims 1-20 were rejected under 35 U.S.C. §103(a) as being unpatentable over Mamros et al., U.S. Patent No. 6,360,269 ("Mamros") in view of an IBM Technical Disclosure Bulletin entitled "Heuristic Method for Grouping Based on Traffic Counts" ("IBM TDB"). Appellant respectfully disagrees for at least the following reasons.

Claims 1 and 9 of the present invention requires the prediction of exchanges of a "specific quantity of communication traffic between network elements" by, among other things, "calculating a weighted traffic flow per usage for a given network element and a comparison of "the value of said weighted traffic flow usage with a remainder value of said specific quantity of communication traffic yet to be processed." Claim 18 adds the feature that the traffic may be "so-called security association (SA).

Said another way, the present invention involves the comparison of traffic which has been processed with a value which represents an amount of traffic that can be processed based on a specific quantity of traffic (e.g., a so-called security association, SA) that can be exchanged between network elements.

As the Final Office Action points out, Mamros does not teach or disclose such a comparison. To overcome this deficiency, the Final Office Action relies on the IBM TDB. However, the IBM TDB is not related to the prediction of exchanges of a specific quantity of traffic between network elements as is required by the claims. Instead, the IBM TDB is directed at a method of grouping nodes in a massive node server system. It is wholly unrelated to the determination or prediction of the exchange of a specific quantity of traffic between network elements, as is required by claims of the present invention.

It appears to the Appellant that the Examiner has ignored the preamble of claims 1, 9 and 18 in determining patentability of the claims. This is impermissible when, as here, "the preamble is 'necessary to give life, meaning, and vitality' to the claim (see *MPEP §2111.02* and cases cited therein) and helps define the inventions in claims 1, 9 and 18. *Id.*

Further, Appellant respectfully submits that the combination of these two references is inappropriate because their combination would render one or both of the references unsatisfactory for their intended purposes or require one or both of the references to change their principle of operation. For example, the IBM TDB is wholly unrelated to the issue of the exchange of security associations used in encrypting data. Therefore, the principle of operation of the heuristic methods in the IBM TDB would have to be changed such that they could be applied to the encryption of data. Alternatively, the principle of operation of Mamros would have to be changed such that it could be used to heuristically group nodes, which is the aim of the IBM TDB. Neither are permissible (see MPEP 2143.01).

Appellant notes the comments contained in the Advisory Action dated August 5, 2005. With respect to the issue of whether it is proper to combine Mamros and the IBM TDB references, it does not appear to Appellant that the Examiner has addressed the substantive, subject matter issues raised by Appellant. For example, the Examiner has not provided any evidence, affidavit

or explanation that would show that one skilled in the art could possibly modify a heuristic method of grouping nodes in a massive node server system (i.e., the IBM TDB) to work with data encryption techniques (in Mamros). Instead, the Advisory Action cites general caselaw and relies on earlier, non-evidentiary Examiner arguments.

Appellant notes that claims 2-8, 10-17, 19 and 20 depend on one of the independent claims and are patentable over Mamros taken separately or in combination with IBM TBD for the reasons set forth above.

VIII. CONCLUSION:

Accordingly, Appellant respectfully requests that the members of the Board reverse the decision of the Examiner and allow claims 1-20.

The Commissioner is authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By: ______________________

John E. Curtin, Reg. No. 37.602
P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

JEC:psy

CLAIMS APPENDIX

Claims 1-20 on Appeal:

1. (Original) An apparatus for use in predicting exchanges of a specific quantity of communication traffic between network elements, said apparatus comprising:

a digital processor operable on a periodic basis to calculate a weighted traffic flow per usage for a given network element, said digital processor further including,

a comparison mechanism for comparing a value of said weighted traffic flow per usage with a remainder value of said specific quantity of communications traffic yet to be processed by said network element, wherein an indication is given by said network element if said remainder value is less than said weighted traffic flow.

2. (Original) The apparatus of Claim 1, wherein said digital processor waits until beginning another time period to calculate another value of said weighted traffic flow per usage to be compared with an updated remainder value.

3. (Original) The apparatus of Claim 1, wherein said specific quantity of communications traffic corresponds to a quantity value associated with a security association (SA) between said network elements.

4. (Original) The apparatus of Claim 3, wherein said indication given from said network elements prompts renegotiation of another SA.

5. (Original) The apparatus of Claim 3, wherein said SA is an Internet Protocol Security (IPSEC) SA.

6. (Original) The apparatus of Claim 1, wherein said apparatus is used in connection with a communications traffic monitoring application to identify randomly occurring traffic patterns.

7. (Original) The apparatus of Claim 1, wherein said apparatus is used in connection with a communications network management application to monitor usage of network components.

8. (Original) The apparatus of Claim 1, wherein said weighted traffic flow per usage corresponds to the average use of network element per period multiplied by the average communications traffic quantity per use.

9. (Original) A method of predicting exchanges of a specific quantity of communication traffic between network elements, said method comprising:

calculating on a periodic basis a weighted traffic flow per usage for a given network element;

comparing a value of said weighted traffic flow per usage with a remainder value of said specific quantity of communications traffic yet to be processed by said network element; and

giving an indication from said network element if said remainder value is less than said weighted traffic flow.

10. (Previously Presented) The method of Claim 9, further including waiting until beginning another time period to calculate another value of said weighted traffic flow per usage to be compared with an updated remainder value.

11. (Original) The method of Claim 9, wherein said specific quantity of communications traffic corresponds to a quantity value associated with a security association (SA) between said network elements.

12. (Original) The method of Claim 11, wherein said indication given from said network elements prompts renegotiation of another SA.

13. (Original) The method of Claim 11, wherein said SA is an Internet Protocol Security (IPSEC) SA.

14. (Original) The method of Claim 1, wherein said method is used in connection with a communications traffic monitoring application to identify randomly occurring traffic patterns.

15. (Original) The method of Claim 9, wherein said method is used in connection with a communications network management application to monitor usage of network components.

16. (Original) The method of Claim 9, wherein said weighted traffic flow per usage corresponds to the average use of network element per period multiplied by the average communications traffic quantity per use.

17. (Original) The method of Claim 9, wherein at least a portion of said communications traffic flows between network elements over the public Internet.

18. (Original) A method of predicting expiration of quantity based security associations between network elements, at least a portion of communications traffic exchanged between said network flowing over the public Internet, said method comprising:

calculating on a periodic basis a weighted traffic flow per usage for a given network element;

comparing a value of said weighted traffic flow per usage with a remainder value of yet to be processed communications traffic of one of said quantity based security associations; and

renegotiating another security association with a corresponding one of said network elements if said remainder value is less than said weighted traffic flow.

19. (Original) The method of Claim 18, wherein said weighted traffic flow per usage corresponds to the average use of a security association per period multiplied by the average number of bytes processed per use.

20. (Original) The method of Claim 18, wherein said security association is an IPSEC security association.

FIG. 1

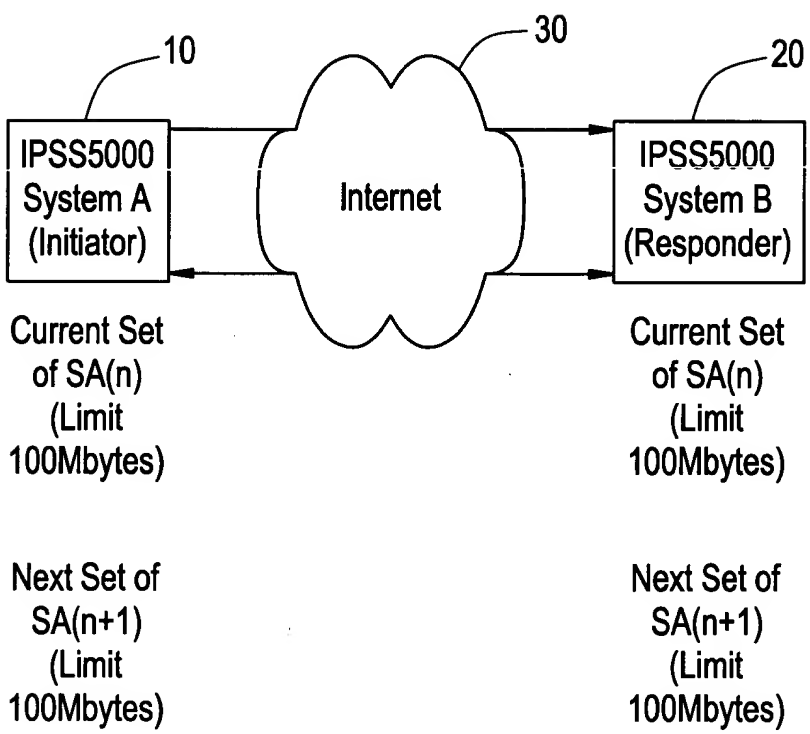

10
30
20
IPSS5000
System A
(Initiator)
Internet
IPSS5000
System B
(Responder)
Current Set
of SA(n)
(Limit
100Mbytes)
Current Set
of SA(n)
(Limit
100Mbytes)
Next Set of
SA(n+1)
(Limit
100Mbytes)
Next Set of
SA(n+1)
(Limit
100Mbytes)

FIG. 2

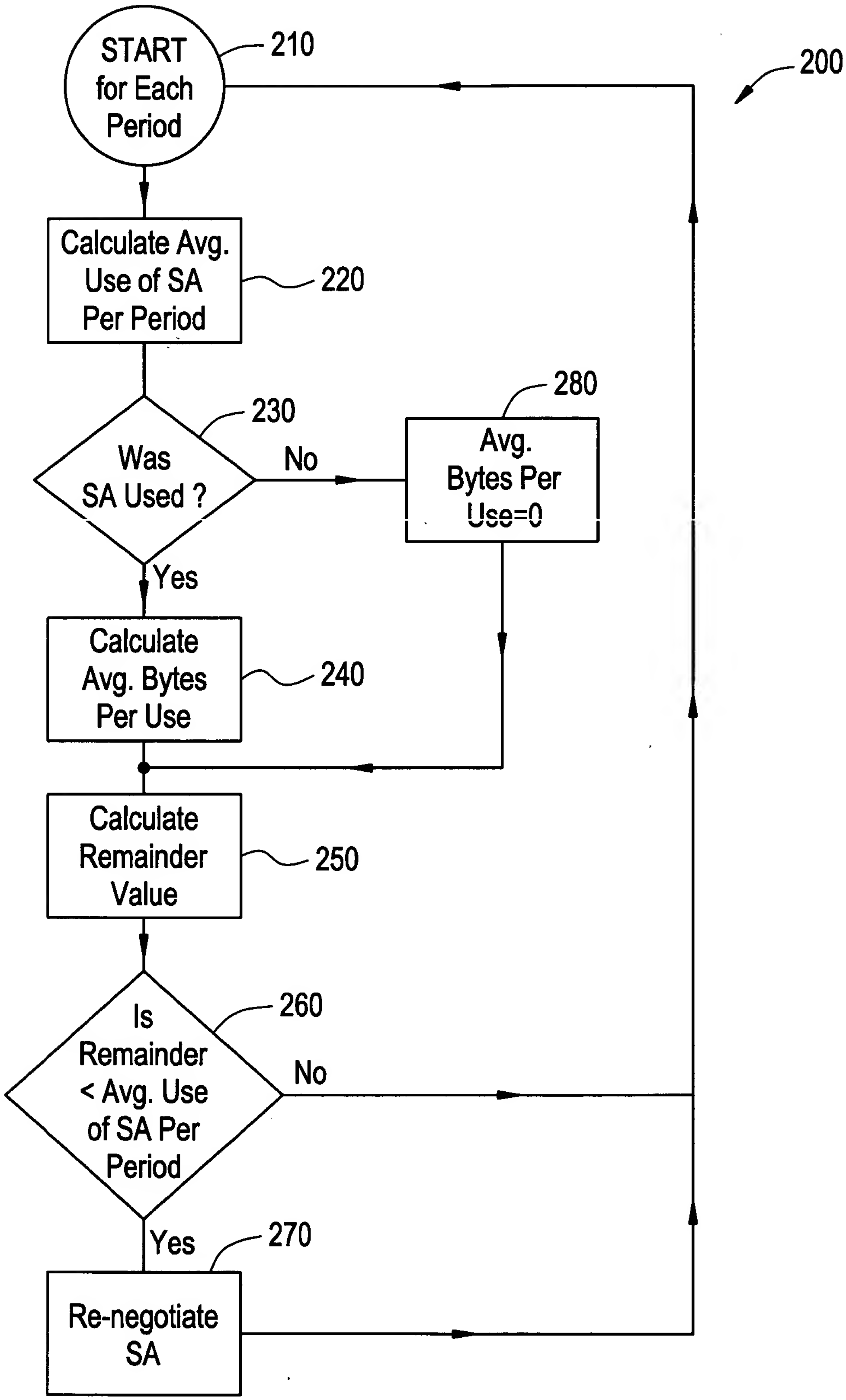
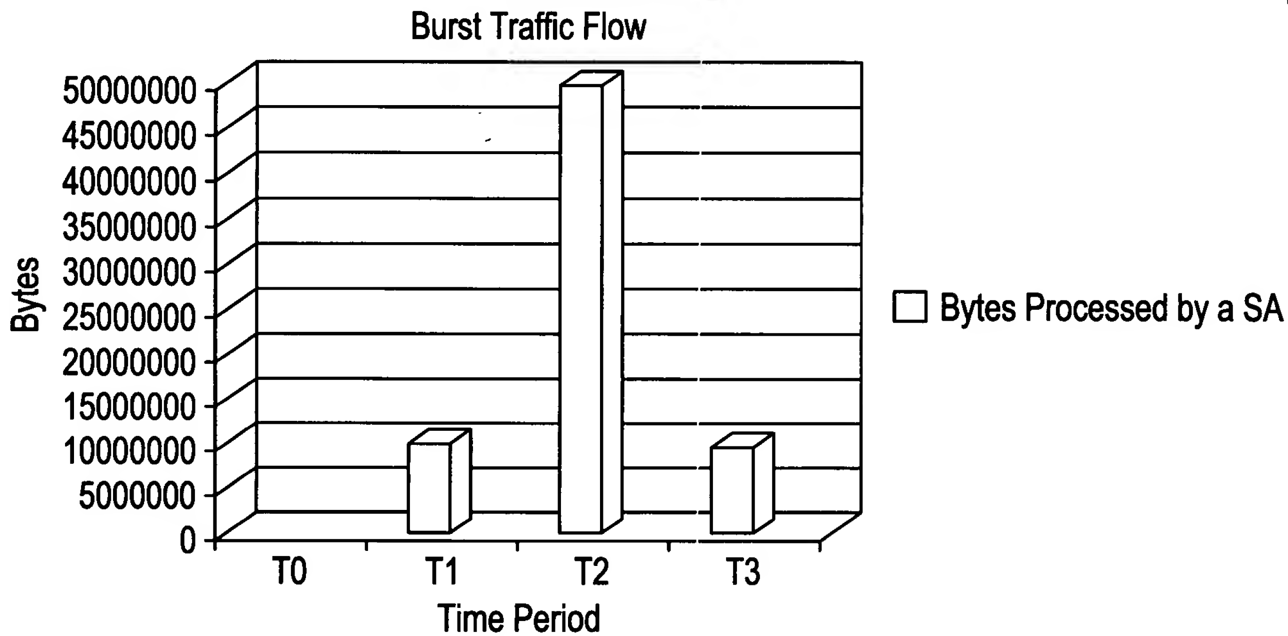

200
START for Each Period
210
Calculate Avg. Use of SA Per Period
220
Was SA Used ?
230
No
Yes
Avg. Bytes Per Use=0
280
Calculate Avg. Bytes Per Use
240
Calculate Remainder Value
250
Is Remainder < Avg. Use of SA Per Period
260
No
Yes
Re-negotiate SA
270

FIG. 3



Period T	Bytes Processed by a SA	Number of Times the SA was used.
T0	0	0
T1	$10 * 10^6$	$10 * 10^3$
T2	$50 * 10^6$	$50 * 10^3$
T3	$10 * 10^6$	$10 * 10^3$

AF IFW

HDP/SB/21 based on PTO/SB/21 (08-00)

Please type a plus sign (+) inside this box → +

O I P E
AUG 3 1 2005
PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	09/771,406
Filing Date	January 26, 2001
Inventor(s)	Abbas BAGASRAWALA
Group Art Unit	2145
Examiner Name	Scott M. Collins
Attorney Docket Number	29250-002065/US

ENCLOSURES *(check all that apply)*

- ☒ Fee Transmittal Form
  - ☒ Fee Attached
- ☐ Amendment
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
- ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Assignment Papers *(for an Application)*
- ☐ Letter to the Official Draftsperson and ______ Sheets of Formal Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) ______
- ☐ After Allowance Communication to Group
- ☐ LETTER SUBMITTING APPEAL BRIEF AND APPEAL BRIEF (w/clean version of pending claims)
- ☒ Appeal Communication to Group (*Notice of Appeal, **Brief**, Reply Brief)*
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) *(please identify below)*:

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm *or* Individual name	Harness, Dickey & Pierce, P.L.C.	Attorney Name John E. Curtin	Reg. No. 37,602
Signature			
Date	August 31, 2005		

PTO/SB/17 (12-04)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

OIPE AUG 3 1 2005 PATENT & TRADEMARK OFFICE

FEE TRANSMITTAL for FY 2005

Effective 10/01/2004. Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 500

Complete if Known	
Application Number	09/771,406
Filing Date	January 26, 2001
First Named Inventor	Abbas BAGASRAWALA
Examiner Name	Scott M. Collins
Art Unit	2145
Attorney Docket No.	29250-002065/US

METHOD OF PAYMENT *(check all that apply)*

☒ Check ☐ Credit card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 08-0750

Deposit Account Name: Harness, Dickey & Pierce, PLC

The Director is authorized to: *(check all that apply)*
☐ Charge fee(s) indicated below ☐ Credit any overpayments
☐ Charge any additional fee(s) during the pendency of this application
☐ Charge fee(s) indicated below, **except for the filing fee**
to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1011	300	2011	150	Utility filing fee	
1012	200	2012	100	Design filing fee	
1013	200	2013	100	Plant filing fee	
1014	300	2014	150	Reissue filing fee	
1005	200	2005	100	Provisional filing fee	

SUBTOTAL (1) ($) 0

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

			Extra Claims		Fee from below		Fee Paid
Total Claims		-20 ** =	0	X		=	0
Independent Claims		-3 ** =	0	X		=	0
Multiple Dependent						=	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	50	2202	25	Claims in excess of 20
1201	200	2201	100	Independent claims in excess of 3
1203	360	2203	180	Multiple dependent claim, if not paid
1204	200	2204	100	** Reissue independent claims over original patent
1205	50	2205	25	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

***or number previously paid, if greater; For Reissues, see above*

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	120	2251	60	Extension for reply within first month	
1252	450	2252	225	Extension for reply within second month	
1253	1020	2253	510	Extension for reply within third month	
1254	1,590	2254	795	Extension for reply within fourth month	
1255	2,160	2255	1080	Extension for reply within fifth month	
1401	500	2401	250	Notice of Appeal	
1402	500	2402	250	Filing a brief in support of an appeal	500
1403	1000	2403	500	Request for oral hearing	
1452	500	2452	250	Petition to revive – unavoidable	
1453	1500	2453	750	Petition to revive – unintentional	
1501	1400	2501	700	Utility issue fee (or reissue)	
1502	800	2502	400	Design issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17 (q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	790	2809	395	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR § 1.129(b))	
1801	790	2801	395	Request for Continued Examination (RCE)	

Other fee (specify) ____

***Reduced by Basic Filing Fee Paid** SUBTOTAL (3) ($)500

4. SEARCH/EXAMINATION FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1111	500	2111	250	Utility Search Fee	
1112	100	2112	50	Design Search Fee	
1113	300	2113	150	Plant Search Fee	
1114	500	2114	250	Reissue Search Fee	
1311	200	2311	100	Utility Examination Fee	
1312	130	2312	65	Design Examination Fee	
1313	160	2313	80	Plant Examination Fee	
1314	600	2314	300	Reissue Examination Fee	

SUBTOTAL (4) ($)0

SUBMITTED BY				Complete (if applicable)	
Name (Print/Type)	John E. Curtin	*Registration No. (Attorney/Agent)*	37,602	*Telephone*	(703) 668-8000
Signature				*Date*	August 31, 2005

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.